

DO NOT ENTER: /M.H./

**IN THE U.S. PATENT AND TRADEMARK OFFICE**

In re U.S. Patent Application of:

APPLICANT: Franck LE et al.

SERIAL NO.: 10/721,504                      FILING DATE: November 26, 2003

EXAMINER: Matthew T. Henning      ART UNIT: 2431

ATTORNEY'S DOCKET NO.: 800.0186.U1(US)

TITLE: Security for Protocol Transversal

Mail Stop AF  
Commissioner for Patents  
P.O. BOX 1450  
Alexandria, VA 22313-1450

**RESPONSE TO OFFICE ACTION**

Sir:

This paper is herewith filed in response to the Examiner's final Office Action mailed on 11 June 2010 for the above-captioned U.S. Patent Application. This paper is deemed to be filed within the shortened statutory period, and no petition or fee for an extension of time is required. However, should the undersigned attorney be mistaken, please consider this a petition for any extension of time that may be required to maintain the pendency of this Patent Application, and charge deposit account no.: 50-1924 for any required fee deficiency.

Please amend the application as shown on the following sheets.

### IN THE CLAIMS

This listing of the claims will replace all prior versions, and listings, of the claims in this application.

1. (Currently Amended) A method, comprising:  
generating validity information for a packet, wherein the validity information comprises all necessary information required to perform a validity check of the packet, the validity information comprising algorithm information to be used to perform the validity check of the packet and algorithm initialization information, the validity information further comprising public key information of a sending node comprising an ~~identity of an entity~~ address in a database of a server from which the public key of the sending node can be obtained, where no pre-established security association is needed to verify the packet;  
  
generating a packet header, comprising the validity information; and  
  
sending the packet including the packet header from a first network node to a second network node.
2. (Previously Presented) The method according to claim 1, wherein the generating of the validity information comprises generating security information indicating security services applied to the packet.
3. (Cancelled)

4. (Previously Presented) The method according to claim 1, wherein the generating of the algorithm information comprises generating the algorithm information which indicates an algorithm to be used to perform the validity check of the packet.

5.-10. (Cancelled).

11. (Previously Presented) The method according to claim 1, wherein the generating of the public key information comprises generating public key verification information indicating information in order to verify that the public key actually belongs to the sending node.

12. (Previously Presented) The method according to claim 1, wherein the generating of the validity information comprises generating an information item to prevent replay attacks.

13. (Previously Presented) The method according to claim 12, wherein the generating of the information item comprises including in the information item an indication of a procedure to be used for anti replay attacks.

14. (Previously Presented) The method according to claim 12, wherein the generating of the information item comprises including in the information item a time stamp.

15. (Previously Presented) The method according to claim 1, further comprising:  
signing the packet using a private key corresponding to the public key indicated by the validity information.

16-17. (Cancelled)

18. (Currently Amended) An apparatus, comprising:
- validity information generating means for generating validity information for a packet;
  - packet header generating means for generating a header for the packet, comprising the validity information; and
  - sending means for sending the packet including the header to a receiving network node,
- wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising ~~address in a database of a server~~ ~~an identity of an entity~~ from which the public key of the sending node can be obtained.

19.-41. (Cancelled)

42. (Currently Amended) An apparatus, comprising:
- a validity information generator configured to generate validity information for a packet;
  - a packet header generator configured to generate a header for the packet, comprising the validity information; and

a transmitter configured to send the packet including the header to a receiving network node,

wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising ~~an identity of an entity~~ address in a database of a server from which the public key of the sending node can be obtained.

43. (Previously Presented) The apparatus according to claim 42, wherein the validity information comprises security information indicating security services applied to the packet.

44.-49. (Cancelled)

50. (Previously Presented) The apparatus according to claim 42, wherein the public key information comprises public key verification information indicating information in order to verify that the public key actually belongs to the sending node.

51. (Previously Presented) The apparatus according to claim 42, wherein the validity information comprises an information item to prevent replay attacks.

52. (Previously Presented) The apparatus according to claim 51, wherein the information item to prevent replay attacks contains an indication of a procedure to be used for anti-replay attacks.
53. (Previously Presented) The apparatus according to claim 51, wherein the information item to prevent replay attacks contains a time stamp.
54. (Previously Presented) The apparatus according to claim 42, further comprising:  
a signor configured to sign the packet using a private key corresponding to a public key indicated by the validity information in the packet header in the sending network node.
55. (Currently Amended) An apparatus, comprising:  
a receiver configured to receive packets from a sending network node; and  
a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet,  
wherein the validity information comprises all necessary information required to perform the validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising an ~~address in a database of a server~~~~identity of an entity~~ from which the public key of the sending node can be obtained.

56. (Previously Presented) The apparatus according to claim 55, wherein the validity information comprises security information indicating security services applied to the packet.

57.-58. (Cancelled)

59. (Currently Amended) An apparatus, comprising:

a transmitter configured to forward packets from a sending network node to a receiving network node; and

a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet,

wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising an address in a database of a server identity of an entity from which the public key of the sending node can be obtained.

60. (Previously Presented) The apparatus according to claim 59, wherein the validity information comprises security information indicating security services applied to the packet.

61.-62. Cancelled.

63. (Currently Amended) A method, comprising:

receiving packets at a network node; and

performing a validity check of a packet by referring to validity information contained in a header of the packet,

wherein the validity information comprises all necessary information required for performing the validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising an address in a database of a server entity from which the public key of the sending node can be obtained.

64. (Currently Amended) A method, comprising:

forwarding received packets to a network node; and

performing a validity check of a packet by referring to validity information contained in a header of the packet,

wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet, wherein the algorithm information comprises values to initialize an



algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising an address in a database of a serverentity from which the public key of the sending node can be obtained.

65. (Cancelled)

66. (Currently Amended) A non-transitory computer readable storage medium ~~comprising with an executable~~ computer program stored thereon, wherein that when executed controls the computer program instructs a processor to perform:

generating validity information for a packet, wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used to perform the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising an address in a database of a serverentity from which the public key of the sending node can be obtained;

generating a packet header, comprising the validity information; and

sending the packet including the header from a first network node to a second network node.

67. (Currently Amended) A non-transitory computer readable storage medium with ~~comprising an executable~~ computer program stored thereon, wherein that when executed ~~controls the computer program instructs~~ a processor to perform:

receiving packets at a network node; and

performing a validity check of a packet by referring to validity information contained in a header of the packet,

wherein the validity information comprises all necessary information required for performing the validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising an address in a database of a server~~entity~~ from which the public key of the sending node can be obtained.

68. (Currently Amended) A non-transitory computer readable storage medium ~~comprising~~ with an executable computer program stored thereon, wherein that when executed controls the ~~computer program instructs~~ a processor to perform:

forwarding received packets to a network node; and

performing a validity check of a packet by referring to validity information contained in a header of the packet,

wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the

packet, wherein the algorithm information comprises values to initialize an algorithm to be used to perform the validity check of the packet, the validity information further comprising public key information of a sending node comprising an address in a database of a server~~identity of an entity~~ from which the public key of the sending node can be obtained.

## REMARKS

Claims 1, 2, 4, 11-15, 18, 42, 42, 50-56, 59, 60, 63, 64, and 66-68 are pending. All independent claims (1, 18, 42, 59, 63, 64, 66-68) have been amended. These amendments are supported by, e.g., paragraph [0025] of the U.S. Patent Publication no. 2004/0268123 corresponding to the instant application.

### Rejections under 35 U.S.C. §101

The Examiner rejected claims 66-68 because allegedly the claimed invention was directed to non-statutory subject matter. Specifically, the Examiner asserted the following:

22 Claims 66-68 are rejected under 35 U.S.C. 101 because the claimed invention is directed  
23  
24 to non-statutory subject matter. The claims are directed to a "computer readable storage medium  
25 comprising a computer program". In the event that such "computer readable storage media"  
  
1 (hereinafter "media") are intended to be limited to the hardware and software necessary to  
2 transmit, transport, receive and process the computer program in such a manner as to enable the  
3 computer program to act as a computer component and realize its functionality, it is believed that  
4 the claims in question would be directed to patent-eligible subject matter (statutory). However,  
5 no such evidence that the embodiment covered by the claims in question which is directed to the  
6 "media" is limited to inclusion of such hardware and software elements exists. Therefore, it is  
7 believed that the "media" would reasonably be interpreted by one of ordinary skill as the abstract  
8 idea of any portion of a communication, including the forms of energy, *per se*, used in  
9 communications. Absent recitation of the hardware, the claims appear devoid of any physical  
10 articles or objects which may cooperate to achieve some function, and as such are not directed to  
11 a machine. Likewise, absent any such physical article or object, they cannot be directed to a  
12 manufacture. They are clearly not a series of steps or acts themselves, and as such are not a

Outstanding Office Action, pages 3-4.

It is unclear to Applicant as to what the Examiner's argument is. For instance, the preamble of claim 66 prior to the instant amendments recited the following (emphasis added):


A computer readable storage medium comprising a computer program that *when executed controls a processor* to perform:

Thus, the preamble requires a computer program to be executed by a processor, where the executed computer program causes the processor to perform certain operations. It is therefore unclear to the Applicant as to how the Examiner can state that this claim is "devoid of any physical articles or objects which may cooperate to achieve some function", since the claim specifically recites a computer program that, when executed, controls a processor to perform operations.

Nonetheless, Applicant has amended the preambles of claims 66-68 to recite the following (see, e.g., claim 66 in its currently amended state):

A non-transitory computer readable storage medium ~~comprising with an executable computer program stored thereon, wherein that when executed controls the computer program instructs~~ a processor to perform:

The New Interim Patent Subject Matter Eligibility Examination Instructions, dated 24 August 2009 specifically states the following:



## PRODUCT EXAMPLE: CLAIM 3

### Computer-Readable Medium

Claim 3. A non-transitory computer-readable storage medium with an executable program stored thereon, wherein the program instructs a microprocessor to perform the following steps:

- sorting results of a search into groups based on a first characteristic;
- ranking the results based on a second characteristic using a mathematical formula [f], and
- comparing the ranked results to a predetermined list of desired results to evaluate the success of the search.

- Is the claim directed to a manufacture? (P1)
  - YES - it is an article (a non-transitory storage medium) produced from raw or prepared materials.
- Does it recite a judicial exception? (P3)
  - YES - it recites a mathematical algorithm.
- Is it directed to a practical application? (P4)
  - YES - evidenced by the tangible embodiment of the computer-readable storage medium.
- Is the claim directed to substantially all practical applications of the mathematical algorithm? (P5)
  - NO - there are other substantial uses of the algorithm than using it in evaluating search results in a program stored on the particular claimed manufacture. As there are other ways to use the algorithm, for example, with different programmed steps, not every use is covered by the claim.

➤ The claim is **eligible** (P6).

8/25/2009 10

See the presentation “Interim Examination Instructions for Evaluating Subject Matter Eligibility Under 35 U.S.C. §101”, August 2009. Claims 66-68 are similar in structure to Claim 3 shown above in the presentation. In fact, Applicant has amended the preambles of these claims to be substantially identical to the preamble of Claim 3 in the presentation. Therefore, claims 66-68 should be patentable under 35 U.S.C. §101.

It is noted that a second Interim Guidance for Determining Subject Matter Eligibility was issued by the PTO in the Federal Register on 27 July 2010. However, the newly issued Interim Guidance is related to process claims and does not appear to discuss computer readable product claims. Therefore, the previous New Interim Patent Subject Matter Eligibility Examination Instructions, dated 24 August 2009, should still be controlling.

For at least these reasons, the 35 U.S.C. §101 rejections to claims 66-68 should be withdrawn.

35 U.S.C. §103(a) Rejections

The Examiner rejected claims 1, 2, 15, 18, 42, 43, 54-56, 59, 60, 62-64, and 66-68 under 35 U.S.C. §103(a) as being unpatentable over Gupta (U.S. Patent no. 6,389,532) in view of Mitreuter (U.S. Patent Publication no. 2003/033375).

Applicant has similarly amended the independent claims 1, 18, 42, 59, 63, 64, 66-68. Claim 1 is illustrative (claim 1 is shown in its currently amended form):

1. A method, comprising:

generating validity information for a packet, wherein the validity information comprises all necessary information required to perform a validity check of the packet, the validity information comprising algorithm information to be used to perform the validity check of the packet and algorithm initialization information, the validity information further comprising public key information of a sending node comprising an ~~identity of an entity~~address in a database of a server from which the public key of the sending node can be obtained, where no pre-established security association is needed to verify the packet;

generating a packet header, comprising the validity information; and

sending the packet including the packet header from a first network node to a second network node.

This amendment is supported, e.g., by paragraph [0025] of the U.S. Patent Publication no. 2004/0268123 corresponding to the instant application.

This amendment should be entered, as it reduces issues for appeal and the Examiner has already rejected the language of “further comprising public key information of a sending node comprising an identity of an entity from which the public key of the sending

node can be obtained". In particular, the Examiner states the following in the outstanding Office Action:

9 Further still, if the examiner were to interpret the limitation of "an identity of an entity  
10 from which the public key of the sending node can be obtained" more specifically to mean an  
11 entity outside of the packet or packet header, the claims would still remain obvious in view of  
12 Gupta, Mitreuter, and Yamagishi et al. (US Patent Number 7,136,998). Yamagishi teaches that  
13 in place of a public key certificate itself, a URL where the public key certificate has been put can  
14 be provided, in order to allow the latest public key certificate to be obtained.

Outstanding Office Action, page 3. Because each independent claim has been similarly amended, Applicant will assume that all claims are rejected under a combination of Gupta, Mitreuter, and Yamagishi.

It is respectfully submitted that the alleged combination of Gupta, Mitreuter, and Yamagishi does not disclose all elements of the independent claims. In particular, independent claim 1 and the other independent claims substantially recite the subject matter of "generating validity information for a packet, wherein the validity information comprises all necessary information required to perform a validity check of the packet, the validity information comprising algorithm information to be used to perform the validity check of the packet and algorithm initialization information, the validity information further comprising public key information of a sending node comprising an address in a database of a server from which the public key of the sending node can be obtained, where no pre-established security association is needed to verify the packet".

The Examiner points to Yamagishi for alleged disclosure that an URL (uniform resource locator) can be used to access a public key of a sending node. However, what Yamagishi concerns is PKI (public key infrastructure) storage and updating. See the following from Yamagishi:



Notification of lapse information of a public key certificate from a PKI directory server to a PKI directory client. Certificate authority information in a certificate authority structure is made to correspond to a container entry, end entity information is made to correspond to a leaf entry, and the certificate authority structure is assigned to a directory tree. If a certain certificate is lapsed and a certificate is newly issued, the newly issued certificate and its serial number are stored in the entry. After a predetermined time elapses, the certificate is put into a certain URL and the certificate stored in the entry is replaced with the URL information. At a receiver, a filtering mask is set on the basis of a certificate pass for obtaining the necessary certificate. A directory tree in which URL information and the serial number have been stored is repetitively transmitted from the transmission side. At the receiver, only the entries selected by the filtering mask are updated.

Abstract of Yamagishi. It is believed that URLs are used in Yamagishi so that when an update to a PKI tree is broadcast, the broadcast of the update takes less bandwidth. For example, Yamagishi states the following:

As mentioned above, according to the embodiment, two kinds of forms such as case of directly storing the latest public key certificate and case of storing the information for obtaining the latest public key certificate are provided for the attribute of the entry. By enabling the two kinds of information to be stored for the entry attribute as mentioned above, the broadcast network resources can be effectively used.

Generally, a data size of the public key certificate is much larger than that of the information (**for example, URL, or the like**) for obtaining the certificate. Therefore, **when the directory structure has an extremely large number of directory entries, if the latest public key certificate corresponding to such a large number of directory entries is periodically broadcasted, the band is remarkably suppressed.** However, if the whole information for obtaining the public key certificates is broadcasted in order to save the band, when the latest public key on the reception side is referred to, the process for obtaining the public key certificate through the communication network is certainly performed and a traffic of the communication network is suppressed.

**Therefore, to utilize an advantage of the instantaneous wide band distribution through the broadcast network, the following method is used in the embodiment of the invention.** That is, for example, if a certain public key certificate is lapsed, the public key certificate which was newly issued is stored into the attribute "LatestPublicKeyCertificate" of the corresponding entry and the serial number of the public key certificate is

stored into "PublicKeyCertificateSerialNumber" and they are broadcasted as updating information. When a predetermined time has expired, the public key certificate is put into the address designated by a certain URL. The contents of the attribute "LatestPublicKeyCertificate" of the entry are replaced into the URL and broadcasted as updating information. **By this method, the band can be effectively used.**

Yamagishi, col. 29, line 54 to col. 30, line 22. It is believed what this means is that instead of sending a PKI directory containing the public key certificates, the entry for the latest public key certificate in the directory is replaced by an URL where the certificate is located, and the PKI directory is still repeatedly transmitted but contains a smaller amount of data, since the certificate has been replaced with an URL.

However, Yamagishi relates to transmission of directories and transmission of not messages of data. Furthermore, Mitreuter teaches away from a combination with Yamagishi (emphasis added):

[0022] 5. With the help of his "private key" of an asymmetrical authentication procedure, the sender generates a digital fingerprint of the message to be sent, which then is attached to the message, and he also attaches his electronic certificate to the message. **This certificate contains the "public key"**, and the name of the user. The recipient can verify the digital fingerprint with the help of this public key. The recipient now also needs to verify the certificate. This is done according to standard procedure for certificates. For this purpose, the certificate contains a digital fingerprint of the certificate data, generated with the private key of a certification entity. If the recipient possesses the public key of the certification entity, he can verify the integrity of the user's certificate. Possession of the private key, which has been used for the generation of the digital fingerprint of the message, authenticates the user.

Thus, Mitreuter specifically discloses and implies that the public key can be placed directly in a message, and one skilled in the art would not look to Yamagishi to add transmission of PKI directories containing URLs to Mitreuter.

Further, in Gupta, the public keys are installed into DNS servers or certification servers and are not sent in messages:

In an embodiment consistent with the present invention, owner 106 creates and distributes public and private keys. An embodiment consistent with this method is shown in FIG. 5 and generally designated 500. In step 502, owner 106 creates several public and private key pairs for a multicast and stores them in indexed tables. In step 504, owner 106 obtains a private multicast address. **Next, in step 506, owner 106 installs the public keys for the multicast. Owner 106 may install the public keys in the DNS server 412 or in a certification server.** After installing the public keys, owner 106 distributes private (secret) keys to authorized senders, in step 508. Note that owner 106 may change which senders are authorized by sending a replacement key to a new set of authorized senders and by disallowing use of the current key. If there are multiple private keys, an index is associated with each key. As shown in FIG. 2, both public key table 216 (in the DNS server) and private key table 236 (in the sender) can be indexed. At step 510, the sender is ready to begin.

Gupta, col. 6, lines 8-24 (emphasis added). Therefore, one skilled in the art would not be motivated to send a public key in a message (such as in Mitreuter) because in Gupta public keys are not sent in messages.

Thus, the combination of Gupta, Mitreuter, and Yamagishi is invalid and also does not disclose or imply at least the subject matter of “generating validity information for a packet, wherein the validity information comprises all necessary information required to perform a validity check of the packet, the validity information comprising algorithm information to be used to perform the validity check of the packet and algorithm initialization information, the validity information further comprising public key information of a sending node **comprising an address in a database of a server from which the public key of the sending node can be obtained**, where no pre-established security association is needed to verify the packet” in claim 1 and the other independent claims 18, 42, 59, 63, 64, 66-68. Thus, independent claims 1, 18, 42, 59, 63, 64, 66-68 are patentable over the (invalid) combination of Gupta, Mitreuter, and Yamagishi.

The Examiner rejected claims 4, 12-14, and 51-53 over Gupta in view of Mitreuter and in further view of Naudus (U.S. Patent No. 6,202,081).

Because independent claims 1, 18, 42, and 59 are patentable, their dependent claims 2, 4, 11-15, 43, 50-54, and 60 are patentable for at least the same reasons.

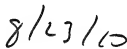
Conclusion

Based on the foregoing arguments, it should be apparent that all remaining claims are thus allowable over the reference(s) cited by the Examiner, and the Examiner is respectfully requested to reconsider and remove the rejections. The Examiner is invited to call the undersigned attorney for any issues.

Respectfully submitted:



Robert J. Mauri  
Reg. No.: 41,180



Date

Customer No.: 29683

HARRINGTON & SMITH, Attorneys at Law, LLC  
4 Research Drive  
Shelton, CT 06484-6212

Telephone: (203)925-9400  
Facsimile: (203)944-0245  
email: rmauri@hspatent.com

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450 or is being transmitted electronically to the United States Patent and Trademark Office.

S.N. 10/721,504  
Art Unit: 2431

Clair F. Mian

Name of Person Making Deposit

8/23/2010

Date